Insecure Default Configuration in P4 Server

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-6043
State	PUBLISHED
Assigner	Perforce
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 12:17:07 UTC
Updated	2026-04-28 13:19:22 UTC
Description	P4 Server versions prior to 2026.1 are configured with insecure default settings that, when exposed to untrusted networks,

Risk And Classification

Primary CVSS: v4.0 8.8 HIGH from security@puppet.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000210000 probability, percentile 0.058270000 (date 2026-04-26)

Problem Types: CWE-1188 | CWE-1188 CWE-1188 Initialization of a resource with an insecure default

Version	Source	Type	Score	Severity	Vector
4.0	security@puppet.com	Secondary	8.8	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:X
4.0	CNA	CVSS	8.8	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

ntegrity

Low

vailability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Perforce	Helix Core Server P4D	affected 2025.2 custom	Not specified

References

Reference	Source	Link	Tags
help.perforce.com/helix-core/server-apps/p4sag/current/Content/P4SAG/secure-by-...	security@puppet.com	help.perforce.com	
portal.perforce.com/s/cve/a91Qi000002wRUvIAM/insecure-default-configuration-in-p4...	security@puppet.com	portal.perforce.com	
help.perforce.com/helix-core/server-apps/p4sag/current/Content/P4SAG/security-c...	MITRE	help.perforce.com	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2026-05-14T11:16:00.000Z	Planned release of P4 Server 2026.1 with secure-by-default fix

Solutions

CNA: Upgrade to P4 Server (P4D) version 2026.1 or later, expected in May 2026, which enforces secure-by-default configurations on both new installations and upgrades.

Workarounds

CNA: For installations that cannot immediately upgrade to 2026.1, administrators should apply manual hardening by configuring security-related server settings as documented at https://help.perforce.com/helix-core/server-apps/p4sag/current/Content/P4SAG/security

https://help.perforce.com/helix-core/server-apps/p4sag/current/Content/P4SAG/security-configurables.html.

There are currently no legacy QID mappings associated with this CVE.